Perancangan Kriptografi *Block Cipher* Berbasis CBC (*Cipher Block Chaining*) Termodifikasi dalam Pengamanan Data Lokasi pada *Database Server* Aplikasi *MeetApss*

Artikel Ilmiah

Peneliti:

Fahrizal Ahmad (672010051)
Drs. Prihanto Ngesti Basuki, M.Kom.
Ir. Christ Rudianto, MT.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga

2016

Perancangan Kriptografi *Block Cipher* Berbasis CBC (*Cipher Block Chaining*) Termodifikasi dalam Pengamanan Data Lokasi pada *Database Server* Aplikasi *MeetApss*

Artikel Ilmiah

Diajukan kepada
Fakultas Teknologi Informasi
untuk memperoleh gelar Sarjana Komputer

Peneliti:
Fahrizal Ahmad (672010051)
Drs. Prihanto Ngesti Basuki, M.Kom.
Ir. Christ Rudianto, MT.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen SatyaWacana
Salatiga

2016

Lembar Pengesahan

Judul Tugas Akhir	**: Perancangan Kriptografi *Block Cipher* Berbasis CBC Termodifikasi dalam Pengamanan Data Lokasi pada *Database Server* Aplikasi *MeetApps***
Nama Mahasiswa	**: Fahrizal Ahmad**
NIM	**: 672010051**
Program Studi	**: Teknik Informatika**
Fakultas	**: Teknologi Informasi**

Menyetujui,

Drs. Prihanto N. Basuki, M.Kom	Ir. Christ Rudianto, MT.
Pembimbing 1	Pembimbing 2

Mengesahkan,

Dr. Dharmaputra T. Palekahelu, M.Pd.	Suprihadi, S.Si., M.Kom.
Dekan	Ketua Program Studi

Dinyatakan Lulus Ujian tanggal: 6 Juni 2016

Penguji:

1. M. A. Ineke Pakereng, M.Kom.
2. Alz Danny Wowor, S.Si., M.Cs.

Perancangan Kriptografi *Block Cipher* Berbasis CBC Termodifikasi dalam Pengamanan Data Lokasi pada *Database Server* Aplikasi *MeetApps*

Oleh,

Fahrizal Ahmad
NIM : 672010051

ARTIKEL ILMIAH

Diajukan Kepada Program Studi Teknik Informatika guna memenuhi sebagian dari persyaratan untuk mencapai gelar Sarjana Komputer

Disetujui oleh,

Drs. Prihanto N. Basuki, M.Kom
Pembimbing 1

Ir. Christ Rudianto, MT.
Pembimbing 2

Diketahui oleh,

Dr. Dharmaputra T. Palekahelu, M.Pd.
Dekan

Suprihadi, S.Si., M.Kom.
Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2016

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : FAHRIZAL AHMAD
NIM : 672010051 Email : FAHRIZALAHMAD11@gmail.com
Fakultas : FTI Program Studi : TEKNIK INFORMATIKA
Judul tugas akhir : PERANCANGAN KRIPTOGRAFI BLOCK CIPHER BERBASIS CBC (CIPHER BLOCK CHAINING) TERMODIFIKASI DALAM PENGAMANAN DATA LOKASI PADA DATABASE SERVER APLIKASI MEETAPPS

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-ekslusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 22 JUNI 2016

FAHRIZAL AHMAD
Tanda tangan & nama terang mahasiswa

Mengetahui,

Drs. Prihanto N. Basuki, M.Kom.
Tanda tangan & nama terang pembimbing I

Ir. Christ Rudianto, MT
Tanda tangan & nama terang pembimbing II

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
Jalan Diponegoro 52 – 60
Phone. (0298) 321212 (Hunting)
Fax. (0298) 321433
E-mail: fti@uksw.edu
Salatiga 50711 – INDONESIA

LEMBAR PERSETUJUAN PUBLISH JURNAL

Dengan mempertimbangkan isi dari jurnal mahasiswa :

Nama Mahasiswa : Fahrizal Ahmad
NIM : 672015051

Maka jurnal ini dinyatakan :

LAYAK TERBIT / TIDAK LAYAK TERBIT

Menyetujui,

(.....)
Pembimbing 1

(.....)
Pembimbing 2

Mengetahui,

(M.A. INEKE PAKERENG, M.Kom.)
Penguji 1

(ALZ DANNY WOWOR, S.Si., M.Cs.)
Penguji 2

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA
Jl. Diponegoro 52 - 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 - 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : FAHRIZAL AHMAD

NIM : 672010051 Email : FAHRIZALAHMAD17@gmail.com

Fakultas : FTI Program Studi : Teknik Informatika

Judul tugas akhir : PERANCANGAN KRIPTOGRAFI BLOCK CIPHER BERBASIS CBC (CIPHER BLOCK CHAINING) TERMODIFIKASI DALAM PENGAMANAN DATA LOKASI PADA DATABASE SERVER APLIKASI MEET APPS

Pembimbing : 1. Drs. Prihanto N. Basuki, M.Kom.

2. Ir. Christ Rudianto, MT.

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 22 JUNI 2016

FAHRIZAL AHMAD

Tanda tangan & nama terang mahasiswa

Perancangan Kriptografi *Block Cipher* Berbasis CBC (*Cipher Block Chaining*) Termodifikasi dalam Pengamanan Data Lokasi pada *Database Server* Aplikasi *MeetApss*

[1] Fahrizal Ahmad, [2] Prihanto Ngesti Basuki, [3]Christ Rudianto
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
Email: 1) 672010051@student.uksw.edu, 2) ngesti@staff.uksw.edu,
3) Chris.Rudianto@staff.uksw.edu

Abstract

In system location sharing or sharing locations, someone's position can only be known by certain people. Just as in the MeetApps application where users can only view the location of a person involved in the meeting, but the location data that is stored on a database server MeetApps application does not accompanied by the data protection security system, so the data is vulnerable to fraud / unknown others who are not interested. Therefore it is necessary cryptography as data security location. This research will implement cryptographic techniques CBC block cipher modification (Cipher Block Chaining) used for data security applications MeetApps, with the goal of keeping the data stored on the database server is secure and can't be known by unauthenticated.

Keywords*: cryptography, a block cipher, CBC (Cipher Block Chaining), location sharing.*

Abstrak

Dalam sistem *location sharing* atau berbagi lokasi, posisi seseorang hanya boleh di ketahui oleh orang-orang tertentu. Seperti halnya dalam aplikasi *MeetApps* dimana pengguna hanya dapat melihat lokasi seseorang yang terlibat dalam pertemuan tersebut, akan tetapi data lokasi yang tersimpan pada database server aplikasi *MeetApps* tidak disertai dengan pengamanan data sistem keamanan, sehingga datanya rentan untuk dicuri/diketahui pihak lain yang tidak berkepentingan. Oleh karena hal itu diperlukan kriptografi sebagai pengamanan data lokasinya. Penelitian ini akan mengimplementasikan teknik kriptografi blok *cipher* modifikasi CBC (*Cipher Block Chaining*) yang digunakan untuk pengamanan data aplikasi *MeetApps*, dengan tujuan agar data yang tersimpan pada *database server* aman dan tidak dapat diketahui oleh yang tidak berkepentingan.

Kata Kunci: Kriptografi, blok *cipher*, CBC (*Cipher Block Chaining*), berbagi lokasi.

---

[1] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Salatiga.

[2] Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

[3] Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

1. Pendahuluan

Dalam sistem *location sharing* atau berbagi lokasi, posisi seseorang hanya boleh diketahui oleh orang-orang tertentu. Seperti halnya dalam aplikasi *MeetApps*, dalam fitur *tracking user* nya pengguna hanya dapat melihat posisi orang yang telah tergabung dalam sebuah pertemuan [1].

Masalah yang muncul dalam aplikasi *MeetApps* adalah data lokasi pengguna yang disimpan pada *database server* tidak disertai dengan pengamanan data, sehingga dapat membuka peluang bagi pihak yang tidak berkepentingan menggunakan informasi tersebut untuk hal yang tidak benar atau merugikan pihak yang terkait dalam pertemuan. Berdasarkan pemahaman tersebut, maka data lokasi pada *database server* perlu diamankan. Oleh karena itu teknik kriptografi diperlukan untuk mengamankan data lokasi yang ada pada *database server*.

Saat ini banyak algoritma kriptografi yang digunakan dalam pengamanan data, salah satunya algoritma kriptografi *block cipher*. Blok cipher merupakan algoritma kriptografi simetrik yang mengenkripsi satu blok plainteks dengan jumlah bit tertentu dan menghasilkan blok ciphertext dengan jumlah bit yang sama [2]. Pada penelitian ini menggunakan Algoritma kriptografi *block cipher* dengan mode *Cipher Block Chaining* (CBC) yang dimodifikasi, dengan harapan pengamanan datanya lebih terjaga. Dalam mode *Cipher Block Chaining* (CBC), setiap blok-blok plainteks di *Exclusive OR* dengan blok kunci sebelumnya sebelum dienkripsi [2].

2. Tinjauan Pustaka

Adapun penelitian terdahulu yang menjadi acuan dalam penelitian ini adalah penelitian berjudul "*Appointment Management* Dengan Memanfaatkan Integrasi Media Sosial Facebook dan *Global Positioning System* (GPS) pada Android" membahas tentang manajemen jadwal pertemuan dengan membagi informasi pertemuan lewat event Facebook dan melakukan tracking terhadap pengguna yang terkait dengan pertemuan dengan berbagi lokasi lewat teknologi *Global Positioning System* (GPS) [1].

Penelitian yang berjudul "Implementasi Mode Operasi *Cipher Block Chaining* (CBC) Pada Pengamanan Data", membahas Membangun perangkat lunak dengan menggunakan mode operasi *Cipher Block Chaining* (CBC) pada pengamanan data dengan mengubah data yang dienkripsi menjadi *ciphertext* [2].

Penelitian yang berjudul *The Design of Rijndael: The Advanced Encryption Standard/Joan Daemon, Vincent Rijmen.* Penelitian ini merupakan penelitian kriptografi *block cipher* yang memenangkan lomba standard kriptografi baru pengganti DES (Standard kriptografi sebelumnya) yang diadakan oleh agensi departemen perdagangan Amerika Serikat [4].

Penelitian dilakukan sekarang ini berbeda dengan penelitian yang telah dilakukan sebelumnya. Sebelumnya pada penelitian penelitian pertama belum

menggunakan teknik kriptografi dalam pengamanan data sehingga saat mudah untuk dicuri atau dimanipulasi datanya, sedangkan pada penelitian kedua telah menerapkan teknik kriptografi mode *Cipher Block Chaining* (CBC) dalam pengamanan datanya. Masalahnya teknik kriptografi yang digunakan masih belum termodifikasi, yang dimana proses enkripsi dan dekripsi datanya masih sederhana, sehingga rentan untuk dikriptanalisis. Oleh karena itu, penelitian ini memodifikasi dengan menambahkan beberapa proses pada *Cipher Block Chaining* (CBC.

Beberapa teori yang digunakan untuk merancang dan sebagai dasar modifikasi kriptografi *cipher block chaining*. Pada bagian ini akan dibahas tentang pengertian dari kriptografi.

Kriptografi sangat berhubungan erat dengan prinsip keamanan, baik itu keamanan pengaksesan data dan jaringan akses serta lain sebagainya. Kriptografi adalah ilmu yang mempelajari bagaimana supaya pesan tetap aman dan tidak dapat dibaca oleh pihak yang tidak berhak *(anauthorized persons)*. Salah satu teknik kriptografi adalah *Cipher Block*. Pada *cipher block* rangkaian *bit-bit* plainteks dibagi menjadi blok-blok *bit* dengan panjang yang sama. Enkripsi (E) diakukan terhadap blok *bit* menggunakan *bit-bit* kunci K yang ukurannya sama dengan ukuran blok plainteks (P). Algoritma enkripsi menghasilkan blok cipherteks (C) yang berukuran sama dengan blok plainteks. Dekripsi (D) dilakukan dengan cara serupa seperti pada enkripsi [8]. Dimana enkripsi dengan kunci dapat dinyatakan dengan Persamaan (1).

$$E_k(\mathrm{P}) = \mathrm{C}. \tag{1}$$

Dan dekripsi dapat dinyatakan dengan Persamaan (2).

$$D_k(\mathrm{C}) = \mathrm{P}. \tag{2}$$

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

1. Kerahasiaan, adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi *cipher*teks.
2. Integritas data, adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah di manipulasi selama pengiriman. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, adalah layanan yang berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus dapat mengontetikasi satu sama lain sehingga ia dapat memastikan sumber pesan.
4. Non-repudiasi, atau nirpenyangkalan adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan melakukan pengiriman atau penerima pesan menyangkal telah mengirim pesan [2].

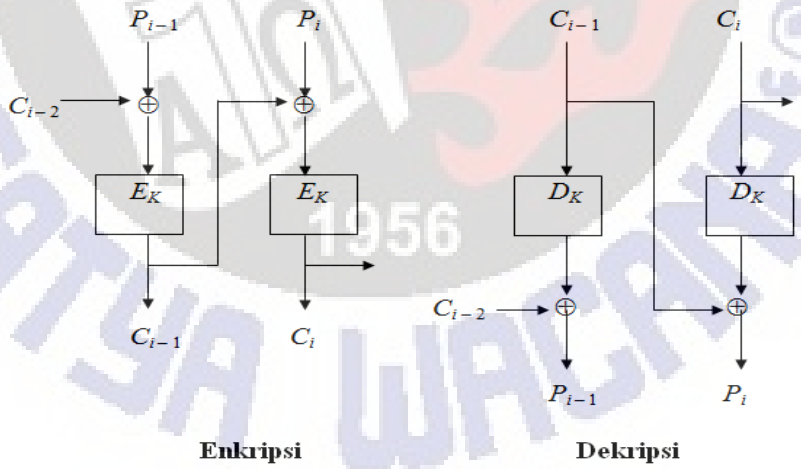
Penelitian ini memodifikasi CBC, dengan demikian harus memenuhi sebagai sebuah sistem kriptografi. Sebuah sistem kriptografi harus memenuhi 5 tuple ***P***, ***C***, ***K***, ***E***, ***D***.

1. ***P*** adalah himpunan plainteks,
2. ***C*** adalah himpunan cipherteks,
3. ***K*** adalah ruang kunci (*keyspace*),
4. ***E*** adalah himpunan fungsi enkripsi $e_k : P \rightarrow C$,
5. ***D*** adalah himpunan fungsi dekripsi $d_k : C \rightarrow P$ [2].

Mode *Cipher Block Chaining* (*CBC*) menerapkan mekanisme umpan-balik (*feedback*) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang *current*. Caranya, blok plainteks yang *current* di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi.

Pada mode *Cipher Block Chaining* (CBC), setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya. Dekripsi dilakukan dengan memasukkan blok cipherteks yang *current* ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya. Dalam hal ini, Blok cipherteks sebelumnya berfungsi sebagai umpan-maju (*feed forward*) pada akhir proses dekripsi.

Pada Gambar 1 memperlihatkan skema proses Enkripsi dan Dekripsi pada Cipher *Block Chaining* (CBC).



Gambar 1 Skema Enkripsi dan Dekripsi dengan mode *CBC.* [2]

Secara matematis, enkripsi dengan *Cipher Block Chaining* (CBC) dinyatakan pada persamaan (3),

$$C_i = E_k(P_i \oplus C_{i-1}) \tag{3}$$

Dan dekripsi dapat dinyatakan dengan Persamaan (4).

$$P_i = D_k(C_i) \oplus C_{i-1} \quad (4)$$

Proses enkripsi metode CBC (*Cipher Block Chaining*) adalah sebagai berikut:

Bagi plainteks menjadi blok-blok yang berukuran 4 bit 1010 0010 0011 1010 1001 atau dalam notasi hexa adalah A23A9. Misalkan kunci (*K*) yang digunakan adalah (panjangnya juga 4 bit) 1011 atau dalam notasi hexa adalah B. Sedangkan IV (*initialization vector*) yang digunakan seluruhnya bit 0 (Jadi, C_0 = 0000).

Misalkan fungsi enkripsi (*E)* yang sederhana adalah dengan meng-XOR-kan blok plainteks P_i dengan *K*, kemudian geser secara *wrapping* bit-bit dari $P_i \oplus K$ satu posisi ke kiri.

C_1 diperoleh sebagai berikut:

$P_1 \oplus C_0$ = 1010 ⊕ 0000 = 1010

Enkripsikan hasil ini dengan fungsi (*E)* sbb:

1010 ⊕ *K* = 1010 ⊕ 1011 = 0001 (C_1)

Geser (*wrapping*) hasil (C_1) satu bit ke kiri: 0010

Jadi, C_1 = 0010 (atau 2 dalam HEX)

C_2 diperoleh sebagai berikut:

$P_2 \oplus C_1$ = 0010 ⊕ 0010 = 0000

0000 ⊕ *K* = 0000 ⊕ 1011 = 1011 (C_2)

Geser (*wrapping*) hasil (C_2) satu bit ke kiri: 0111

Jadi, C_2 = 0111 (atau 7 dalam HEX)

C_3 diperoleh sebagai berikut:

$P_3 \oplus C_2$ = 0011 ⊕ 0111 = 0100

0100 ⊕ *K* = 0100 ⊕ 1011 = 1111 (C_3)

Geser (*wrapping*) hasil (C_3) satu bit ke kiri: 1111

Jadi, C_3 = 1111 (atau F dalam HEX)

Demikian seterusnya hingga semua blok plainteks di XOR, sehingga hasil enkripsi dari plainteks 10100010001110101001 (notasi HEX A23A9), adalah 00100111111111011111 (notasi HEX 27FBF) [2].

Pada metode CBC (*Cipher Block Chaining*) blok plainteks pertama menggunakan C_0 sebagai vektor awal (*initialization vector* atau IV). Blok-blok plainteks yang identik dienkripsi menjadi blok-blok cipherteks yang berbeda hanya jika blok-blok plainteksnya sebelumnya berbeda. Jika blok-blok plainteks sebelumnya ada yang sama, maka ada kemungkinan cipherteksnya sama. Untuk mencegah hal ini, maka digunakan IV yang merupakan data acak sebagai blok pertama. IV tidak mempunyai makna, hanya diguanakan untuk membuat tiap blok cipherteks menjadi unik. Keuntungan Mode *Cipher Block Chaining* (CBC) pesan menjadi jauh lebih aman untuk dideteksi kuncinya karena kunci tiap blok berbeda

beda tergantung dari plainteks sebelumnya. Terlihat bahwa dengan menggunakan mode *CBC*, blok plainteks yang sama (A dalam HEX) dienkripsikan menjadi dua blok cipherteks yang berbeda (masing-masing 2 dan B) [2].

Setelah proses enkripsi dilakukan, maka proses selanjutnya adalah merubah *ciphertext* menjadi plainteks, proses ini disebut dengan proses dekripsi. Proses dekripsi merupakan proses kebalikan dari proses enkripsi.

Kebutuhan pengujian untuk mengetahui besaran nilai algoritma kriptografi yang dimodifikasi mampu untuk mengacak plainteks yang dimasukkan maka digunakan nilai keacakannya. Nilai acak dapat diperoleh dari perbandingan selisih dari nilai plainteks terhadap nilai dari cipherteks [5]. Dimisalkan k_i merupakan nilai acak dimana $k_i \rightarrow i = 1 \ldots 16$ dengan plainteks adalah P_i dan cipherteks adalah C_i maka untuk menghitung nilai acak setiap karakter dapat dinyatakan dengan Persamaan (5).

$$k_i = \frac{(p_i - c_i)}{p_i} \tag{5}$$

Berdasarkan persamaan diatas maka dapat ditentukan persamaan untuk mencari rata-rata dari nilai acak dengan Persamaan (6).

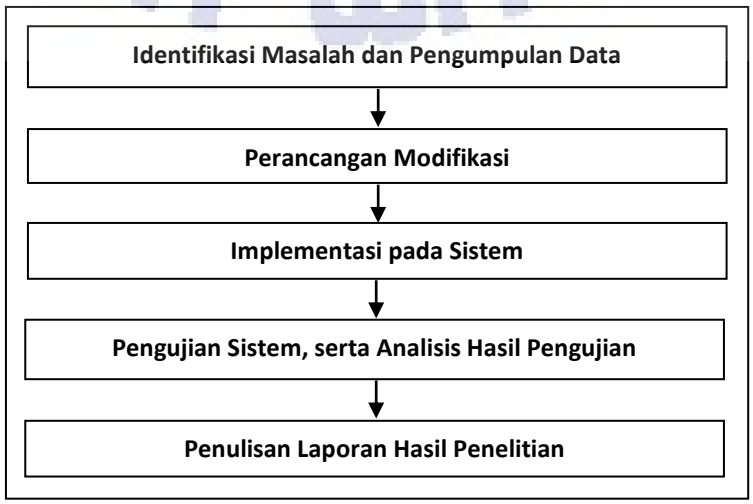
$$\overline{k_l} = \frac{1}{n}\sum_{i=1}^{n} \tag{6}$$

Pada pengujian diferensiasi dimana untuk mengetahui rata-rata tingkat perbedaan dapat ditentukan dengan Persamaan (7).

$$dif = \frac{(c_2 - c_1) + (c_3 - c_2) + \ldots + (c_n - c_{n-1})}{n-1} \tag{7}$$

3. Metode dan Perancangan Sistem

Penelitian yang dilakukan, diselesaikan melalui tahapan penelitian yang terbagi dalam lima tahapan yaitu, (1) Tahap Identifikasi Masalah dan Pengumpulan Data, (2) Perancangan Modifikasi, (3) Implementasi pada Sistem, (4) Pengujian Sistem, serta Analisis Hasil Pengujian, (5) Penulisan Laporan Hasil Penelitian.



Gambar 2 Tahapan Metode Penelitian

Tahapan penelitian pada Gambar 3 dapat dijelaskan sebagai berikut.

1 Identifikasi masalah dan pengumpulan data, yaitu melakukan analisis mengenai masalah yang terjadi dalam penelitian yang dilakukan pada aplikasi *MeetApps*, dimana masih ada kekurangan dalam keamanan data Lokasi pada *database server* dan melakukan pengumpulan data berupa literatur mengenai proses enkripsi, dan dekripsi data menggunakan *CBC* (*Cipher Block Chaining*) untuk proses pengamanan data.

2 Perancangan modifikasi yang meliputi penambahan fungsi atau proses yang baru ke dalam proses enkripsi dan dekripsi pada *CBC* (*Cipher Block Chaining*), kemudian merancang bagan dari proses modifikasi yang di lakukan, serta melakukan analisa-analisa hasil yang dapat diambil dari modifikasi yang telah dilakukan.

3 Implementasi pada sistem, yaitu hasil dari modifikasi teknik kriptografi yang telah dibuat, kemudian diimplementasikan ke dalam aplikasi *MeetApss*.

4 Pengujian sistem serta melakukan analisis hasil pengujian, yaitu mengimplementasikan tahapan penelitian kedua dan ketiga kedalam program, apakah aplikasi dapat bekerja secara optimal sesuai kriteria sistem yang dibangun terkait proses enkripsi dan dekripsi.

5 Penulisan laporan hasil penelitian, yaitu mendokumentasikan proses penelitian yang sudah dilakukan dari tahap awal hingga akhir ke dalam tulisan, yang nantinya menjadi laporan hasil penelitian.

Kebutuhan sistem yang diperlukan untuk tahap uji coba sistem ini adalah kebutuhan yang terdapat pada *smartphone* sebagai wadah implementasi Modifikasi Kriptografi CBC (*Cipher Block Chaining*) dalam proses enkripsi dekripsi yang dimiliki aplikasi ini. Adapun spesifikasi *smartphone* yang dibutuhkan untuk menjalankan aplikasi ini adalah:

1. Sistem operasi android (Jelly Bean) versi 4.1.2 atau di atasnya.
2. Memori minimal 1 GB.

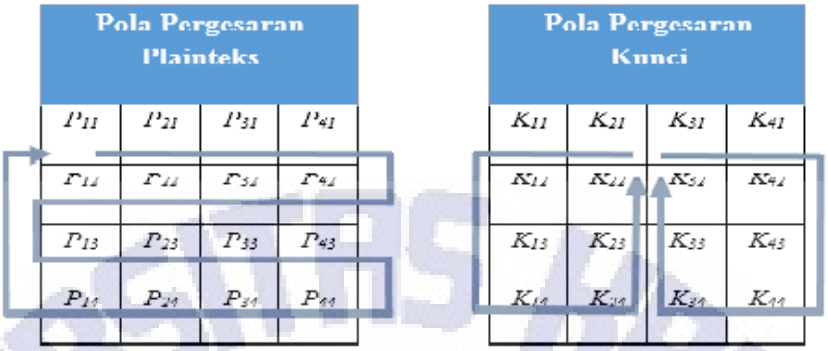
Pada proses enkripsi pada CBC (*Cipher Block Chaining*) melakukan tiga proses untuk yang dijelaskan sebagai berikut: 1) Plainteks dan Kunci diubah menjadi biner, kemudian dibagi menjadi setiap blok-blok *bit*. 2) Menentukan IV (*initialization vector*). 3) Proses *Exclusive OR* dengan IV dan Kunci, sehingga menghasilkan cipherteks.

Pada penelitian ini akan memodifikasi CBC (*Cipher Block Chaining*), dimana modifikasi yang dilakukan yaitu mengubah proses plainteks dan kunci yang dibagi menjadi setiap blok-blok menjadi plainteks dan kunci dimasukan pada state plainteks dan state kunci, kemudian akan melakukan pergeseran (*shifting*) pada state. Dalam modifikasi CBC (*Cipher Block Chaining*) untuk mendapatkan cipherteks ada tiga tahapan utama yang dapat dilakukan seperti masukan plainteks dan kunci dalam state, pergeseran (*shifting*) dengan pola, dan perhitungan *Exclusive* OR dengan IV dan Kunci.

Pada tahap pertama terlebih dahulu plainteks dan kunci diubah menjadi hexa, kemudian disusun secara vertikal ke dalam state plainteks dan kunci yang berukuran 4x4 dimana secara keseluruhan terdapat 128 *bit block* pada setiap state yang bisa dilihat pada Gambar 3.

Gambar 3 State Plainteks dan State Kunci [4].

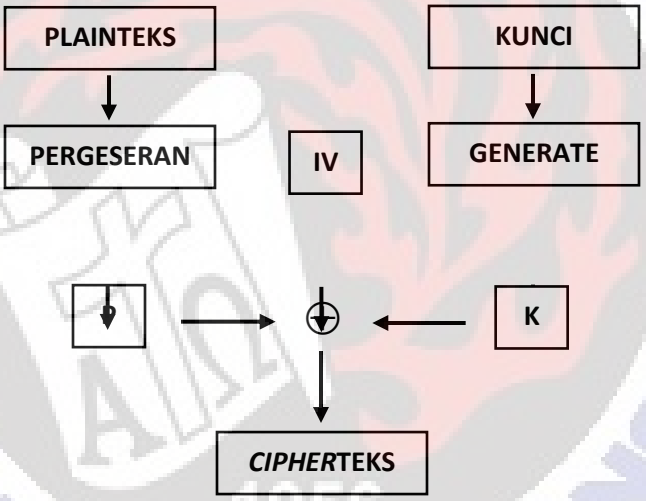
Pada tahapan kedua akan dilakukan proses pergeseran, dimana plainteks dan kunci yang sebelumnya telah disusun dalan state akan digeser sesuai pola yang terlah ditentukan pada setiap statenya yang bisa dilihat pada Gambar 4. Untuk state plainteks pergeseran dimulai dari P_{11}, P_{12}, P_{31}, P_{41} ….., P_{44}, P_{34}, P_{24}, P_{14}, sedangkan untuk state kunci pegeseran dibagi jadi 2 bagian, dimana pada bagian 1 dimulai dari K_{21}, K_{11}, K_{12}, K_{13} ….. K_{23}, K_{22}, kemudian untuk bagian 2 dimulai dari K_{31}, K_{41}, $K4_{2}$, K_{43} ….. K_{33}, K_{32}.



Gambar 4 Pola Pergeseran Plainteks dan Kunci.

Pada tahap terakhir dilakukan perhitungan *Exclusive OR* antara IV dan *bit* kunci.

Secara umum proses enkripsi yang dilakukan pada modifikasi CBC (*Cipher Block Chaining*) dapat dilihat pada Gambar 5.

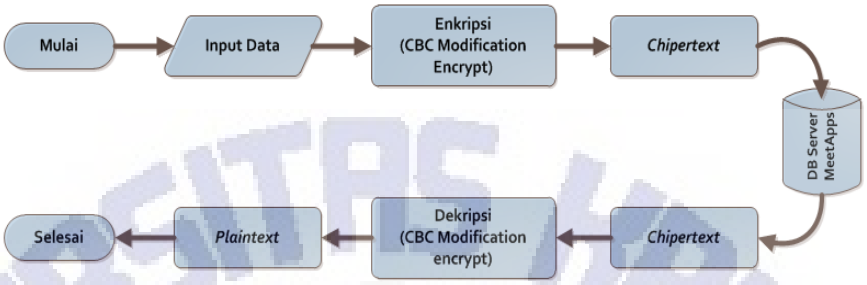


Gambar 5 Bagan Umum Proses Enkripsi Modifikasi CBC.

Gambar 5 merupakan bagan umum proses enkripsi yang terdapat pada pada modifikasi CBC (*Cipher Block Chaining*). Persiapan dan langkah-langkah proses enkripsi perancangan kriptografi dijelaskan sebagai berikut : 1) Menyiapkan plainteks yang akan dienkripsi. 2) Menyiapkan *key* untuk digunakan dalam proses enkripsi. 3) Melakukan proses *generate key*. 4) Melakukan pergeseran pada state plainteks sesuai pola yang ditentukan. 5) Menentukan IV (*initialization vector*). 6) Melakukan *Exlusive OR* terhadap hasil proses plainteks dengan IV dan hasil proses *key*. 6) Menghasilkan cipherteks.

Proses dekripsi merupakan proses yang dilakukan terbalik dengan proses enkripsi. Hanya saja yang menjadi inputan bukan plainteks tetapi cipherteks. Selain

itu juga, kunci yang dimasukkan diregenerasi secara terbalik untuk mengambalikan cipherteks menjadi plainteks.



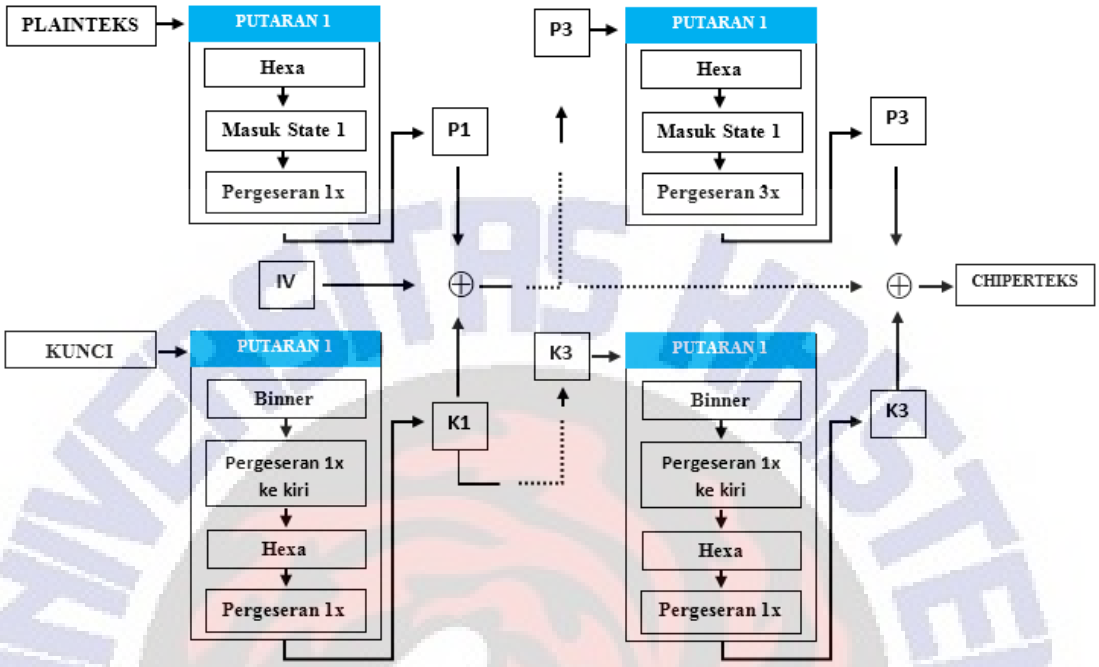
Gambar 6 . Proses Enkripsi dan Dekripsi pada Sistem

Gambar 6 menjelaskan proses enkripsi dan dekripsi yang terjadi pada sistem, dimana proses dimulai dengan input data (data *appointment*), selanjutnya data yang diinputkan akan di enkripsi sesuai dengan langkah-langkah yang ada pada proses enkripsi, sehingga menghasilkan sebuah *cipher*teks yang akan disimpan pada *database server MeetApss*. Untuk proses dekripsi, sistem akan mengambil *cipher*teks yang disimpan pada *database server MeetApss*, selanjutnya akan melakukan dekripsi sesuai dengan langkah-langkah yang ada pada proses dekripsi, sehingga menghasilkan plainteks.

4. Hasil dan Pembahasan

Pada hasil dan pembahasan akan dibahas terlebih dahulu proses enkripsi dan dekripsi secara keseluruhan. Dimana setiap putaran terdiri dari proses plainteks ke-*i* dan juga proses kunci ke-*i*, dengan $i = 1, \ldots, 3$. Proses enkripsi dan dekripsi pada modifikasi CBC (*Cipher Block Chaining*) ini akan melakukan 3 kali proses dari setiap proses pengacakan menggunakan pola yang telah ditentukan, sehingga menghasilkan sebuah cipherteks.

Secara keseluruhan proses enkripsi modifikasi CBC (*Cipher Block Chaining*) dapat dilihat pada Gambar 7.



Gambar 7 Bagan Keseluruhan Proses Enkripsi.

Berdasarkan pada Gambar 7 maka dibahas tiap proses yang ada pada bagan keseluruhan proses enkripsi, dimana disiapkan plainteks "kriptografi" dengan menggunakan kunci "fti-uksw".

Tahap 1:

Susun plainteks dan kunci ke dalam state yang sebelumnya telah diubah ke dalam hexa, akan tetapi karakter pada state kunci diubah ke dalam binner kemudian digeser 1 *bit* ke kiri terlebih dahulu, bisa dilihat pada Gambar 7.

Plainteks			
6B	74	61	
72	6F	66	
69	67	69	
70	72		

Kunci			
66	75		
74	6B		
69	73		
2D	77		

.

Gambar 7 State Plainteks dan State Kunci

Gambar 7 merupakan state plainteks dan state kunci yang telah disusun. Kemudian dilakukan pengecekan apakah plainteks dan kunci telah memiliki panjang yang sama atau belum pada state, jika belum akan di lakukan *padding* hingga memenuhi 128 *bit* blok yang ada pada state plainteks dan kunci. Hasil setelah

dilakukan *padding* (blok abu-abu merupakan bilangan hexa yang ditambahkan/*padding*) bias dilihat pada Gambar 8, sehingga didapatkan persamaan berikut untuk plainteks dan kunci sebagai berikut:

$$P1[p_{11}, p_{12}, p_{13}, p_{14},], \quad K1[k_{11}, k_{21}, k_{31}, k_{41},]$$

$$P2[p_{21}, p_{22}, p_{23}, p_{24},], \quad K2[k_{12}, k_{22}, k_{32}, k_{42},]$$

$$P3[p_{31}, p_{32}, p_{33}, p_{34},], \quad K3[k_{13}, k_{23}, k_{33}, k_{43},]$$

$$P4[p_{41}, p_{42}, p_{43}, p_{44},], \quad K4[k_{14}, k_{24}, k_{34}, k_{44},]$$

Plainteks					Kunci			
6B	74	61	6B		66	75	78	62
72	6F	66	6C		74	6B	79	63
69	67	69	6D		69	73	7A	64
70	72	6A	6E		2D	77	61	65

Gambar 8 *Padding* State Plainteks dan State Kunci

Tahap 2:

Setelah plainteks dan kunci telah memenuhi semua kolom yang ada pada state, selanjutnya dilakukan proses pergeran sesuai pola. Hasil dari pergeseran plainteks dan kunci bisa dilihat pada Gambar 9, sehingga di dapat persamaan setelah pergeseran dapat dilihat sebagai berikut:

$$P1[p_{14}, p_{11}, p_{12}, p_{13},], \quad K1[k_{21}, k_{22}, k_{32}, k_{31},]$$

$$P2[p_{22}, p_{32}, p_{42}, p_{41},], \quad K2[k_{11}, k_{23}, k_{33}, k_{41},]$$

$$P3[p_{12}, p_{13}, p_{23}, p_{33},], \quad K3[k_{12}, k_{24}, k_{34}, k_{42},]$$

$$P4[p_{24}, p_{34}, p_{44}, p_{43},], \quad K4[k_{13}, k_{14}, k_{44}, k_{43},]$$

Plainteks			
70	6B	74	61
6F	66	6C	6B
72	69	67	69
72	6A	6E	6D

Kunci			
EA	D6	F2	F0
CC	E6	F4	F8
E8	EE	F6	FA
D2	5A	FE	FC

Gambar 9 Hasil Pergeseran State Plainteks dan State Kunci

Tahap 3:

Melakukan Proses *Exclusive OR* dimana kolom pertama plainteks akan di *XOR*-kan dengan baris pertama kunci dengan persamaan sebagai berikut:

$$P_i = E_{ki} (P_i \oplus C_i - 1)$$

Proses *xor* pada plainteks kolom pertama dan kunci baris pertama:
IV (*Initialization Vector*) = C_0 = 00001111 (IV dilakukan agar mendapatkan C_0 atau C awal yang akan di *xor*-kan dengan blok plainteks pertama)

$C_1 = P_{11} \oplus C_0 = 01110000 \oplus 00001111 = 01111111$,
$01111111 \oplus K_{11} = 01111111 \oplus 11101010 = 100101001$, hasilnya di geser 1 *bit* ke kiri, $C_1 = 00101011$ atau 2B (hexa).

$C_2 = P_{12} \oplus C_1 = : 01101111 \oplus 00101011 = 01000100$,
$01000100 \oplus K_{21} = 01000100 \oplus 11010110 = 10010010$, hasilnya di geser 1 *bit* ke kiri, $C_2 = 00100101$ atau 25 (hexa).

$C_3 = P_{13} \oplus C_2 = : 01110010 \oplus 00100101 = 01010111$,
$01010111 \oplus K_{31} = 01010111 \oplus 111110010 = 10100101$, hasilnya di geser 1 *bit* ke kiri, $C_3 = 01001011$ atau 4B (hexa).

$C_4 = P_{14} \oplus C_3 = : 01110010 \oplus 01001011 = 00111001$,
$00111001 \oplus K_{41} = 00111001 \oplus 11110000 = 11001001$, hasilnya di geser 1 *bit* ke kiri, $C_4 = 10010011$ atau 93 (hexa).

Demikian seterusnya hingga semua blok plainteks di XOR-kan dengan blok kunci, setelah itu hasil dari $C_1 \ldots C_{16}$ disusun dalam state, kemudian lakukan tahap 1 sampai tahap 3 hingga memenuhi 3 kali putaran, dimana untuk putaran berikutnya proses pergeseran ditambah 1 pada setiap proses dan menghasilkan *ciphertext.* Berdasarkan pengujian dengan "kriptografi" sebagai plainteks dan "fti-uksw" sebagai kuncinya, maka didapat hasil pengujian sebagaimana ditunjukan pada Tabel 1.

Tabel 1 Hasil Enkripsi dan Dekripsi

Plainteks	k	r	i	p	t	o	g	r	a	f	i					
Enkripsi	97	BA	68	95	66	06	85	DC	43	2D	B0	69	E7	CA	B6	69
Dekripsi	k	r	i	p	t	o	g	r	a	f	i					

Berdasarkan hasil proses enkripsi dan dekripsi pada Tabel 1 yang dilakukan menunjukan perancangan modifikasi kriptografi CBC dapat melakukan proses enkripsi dan dekripsi, dimana pada proses enkripsi dan dekripsi dapat merubah plainteks menjadi *cipher*teks yang merupakan nilai hexadecimal, selanjutnya pada proses dekripsi merupakan proses membalikan *cipher*teks menjadi plainteks, sehingga dapat memenuhi kriptosistem.

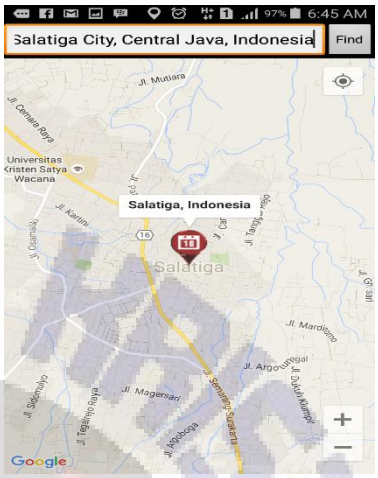
Syarat kriptosistem adalah dapat memenuhi 5 *tuple* (**P, C, K, E, D**), yang dijelaskan sebagai berikut:

1. ***P*** adalah himpunan berhingga dari plainteks, pada rancangan kriptografi ini menggunakan plainteks yang *ekuivalen* dengan karakter ASCII printable. Maka himpunan plainteks pada perancangan kriptografi ini adalah himpunan berhingga.
2. ***C*** adalah himpunan berhingga dari *ciphertext*. *Ciphertext* dihasilkan dalam elemen hexadesimal (1,2,…,9,A,…,F), maka himpunan *ciphertext* yang dihasilkan merupakan elemen terbatas.
3. ***K*** merupakan ruang kunci (*Keyspace*), adalah himpunan berhingga dari kunci. Dimana kunci disetiap putaran merupakan hasil dari pergeseran kunci di putaran sebelumnya. Maka kunci yang digunakan dalam perancangan ini adalah ruang kunci.
4. Untuk setiap $k \in \mathbf{K}$, terdapat aturan enkripsi $e_k \in \mathbf{E}$ dan berko*respond*ensi dengan aturan dekripsi $d_k \in \mathbf{D}$. Setiap $e_k: \mathbf{P} \longrightarrow \mathbf{C}$ dan $d_k: C \longrightarrow P$ adalah fungsi sedemikian hingga $d_k(e_k(x)) = x$ untuk setiap plainteks $x \in \mathbf{P}$.

Kondisi ke-4 ini secara menyeluruh, terdapat kunci yang dapat melakukan proses enkripsi sehingga merubah plainteks menjadi *ciphertext* dan dapat melakukan proses dekripsi yang merubah *ciphertext* ke plainteks. Karena telah memenuhi kelima kondisi, maka rancangan modifikasi kriptografi CBC ini merupakan sebuah sistem kriptografi.

Hasil uji coba aplikasi dilakukan dengan menggunakan *smartphone* SAMSUNG E5 dengan versi android 5.1.1 Lollipop. Hasil yang di peroleh dari uji coba aplikasi dapat dilihat pada tampilan-tampilan aplikasi yang ditunjukan pada gambar-gambar berikut:

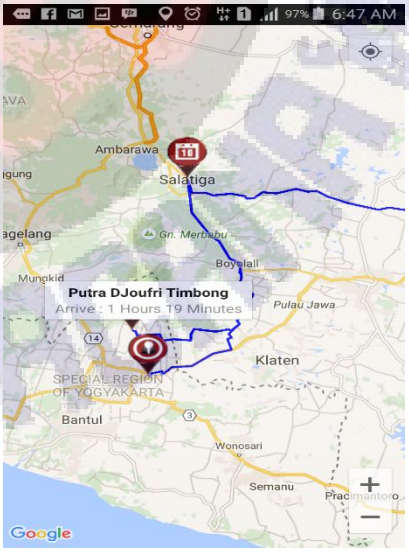
Gambar 10 Membuat Pertemuan



Gambar 11 Cari Lokasi

Membuat pertemuan merupakan tampilan aplikasi dimana *user* akan membuat sebuah pertemuan dengan mengisi detail pertemuan seperti, nama pertemuan, deskripsi pertemuan dan hari dan waktu, yang akan dilakukan seperti yang ditunjukan pada Gambar 10. Pada gambar Cari lokasi, *user* diminta untuk menentukan lokasi pertemuan yang akan dilakukan, dengan mengisi nama lokasi pada *textbox* dan menekan tombol *find*, sehingga aplikasi akan mencari lokasi yang kita imputkan, seperti yang ditunjukan pada Gambar 11.

Gambar 12 Konfirmasi Pertemuan



Gambar 13 *Tracking* posisi

Pada Gambar 12 merupakan halaman dimana *user* mengkonfirmasi pertemuan yang telah dibuat, dimana pada halaman ini juga proses enkripsi akan dilakukan disaat *user* menekan tombol *Yes*, data pertemuan akan dienkripsikan dan disimpan pada *database server MeetApps*. Pada Gambar 13 merupakan halaman *tracking posisi*, *user* dapat melihat posisi pertemuan dan posisi dari seseorang yang telah diundang dalam pertemuan. Pada halaman *tracking* posisi ini pun proses dekripsi akan dilakukan, dimana sebelum lokasi ditampilkan, sistem akan mengambil data lokasi yang telah disimpan pada database server yang berupa *cipher*teks dan di dekripsi.

Hasil enkripsi yang dilakukan pada data lokasi *appoinment* dan data lokasi *user* akan dikirimkan pada *database server* aplikasi *MeetApps*, dimana untuk data *appoitment* di simpan pada *tb_appoinment* yang dibisa dilihat pada Gambar , sedangkan untuk data *user* di simpan pada *tb_tracking*.

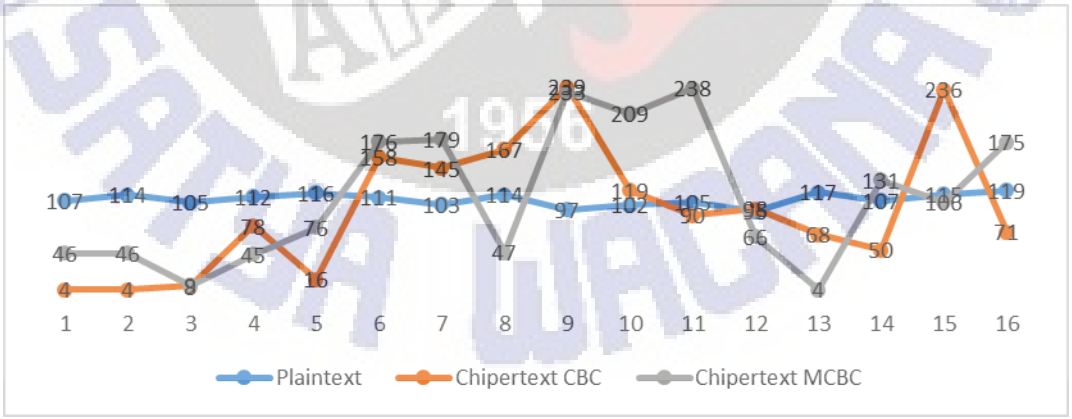
latitude	longitude
9ad9fa605dc1538d5e9dcdbb2bde72da	ab4dbd112806504d9dcd34370e17be93
a3882fcf1b9e9d772e5710de79597d3c	c3ef5186b234f1c9707d4a98aeffc0e4
9ad9fa605dc1538d5e9dcdbb2bde72da	ab4dbd112806504d9dcd34370e17be93

Gambar 14 *tb_Pertemuan*

longitude	latitude
a9edfb47e23ed2faa37d22852b868e5e	f59a5c67d5d082407ac89c091a635459
a9edfb47e23ed2faa37d22852b868e5e	f59a5c67d5d082407ac89c091a635459
a9edfb47e23ed2faa37d22852b868e5e	f59a5c67d5d082407ac89c091a635459

Gambar 15 *tb_Tracking*

Berikut adalah melakukan pengujian pada kriptografi yang dimodifikasi. Pengujian dilakukan untuk mengetahui tingkat keacakan dan nilai diferensial. Hasil pengujian seperti yang ditujukan pada Gambar 16.



Gambar 14 Grafik Perbandingan

Berdasarkan pada Gambar 16 dilakukan analisis tingkat keacakan yang didapat dari selisi cipherteks dengan plainteks dibanding dengan cipherteks. Dimana didapat rata-rata nilai acak CBC adalah 0.094017 dan kriptografi yang dimodifikasi

adalah -0.04844. Hal ini menjelaskan bahwa plainteks cenderung lebih kecil bila dibanding dengan cipherteks dari CBC dan modifikasi teknik kriptografi CBC, dimana cipherteks teknik kriptografi rancangan memberikan nilai cenderung lebih besar dari CBC.

Berikut dilakukan analisis nilai diferensial untuk mengetahui perbedaan karakter sebelum dan sesudah dari cipherteks yang dihasilkan. Berdasarkan persamaan (7) didapat rataan dari nilai diferensial CBC adalah 4.466667 dan kriptografi MCBC adalah 8.6. Berdasarkan hasil tersebut dapat disimpulkan bahwa karakter yang diberikan cipherteks algoritma CBC dan modifikasi CBC (MCBC) yang dibuat memberikan hasil cenderung menurun dari karakter sebelumnya, namun hasil dari MCBC memberikan hasil cenderung lebih menurun dibanding CBC.

5. Simpulan

Berdasarkan penelitian, pengujian, dan analisis terhadap sistem, maka dapat ditarik kesimpulansebagai berikut: (1) Teknik kriptografi modifkasi CBC (*Cipher Block Chaining*) dapat mengamankan data lokasi pada *database server MeetApps;* (2) Modifikasi CBC (*Cipher Block Chaining*) telah menjadi sebuah kriptosistem dengan memenuhi lima tuple; (3) Proses modifikasi CBC (*Cipher Block Chaining*), dapat mengenkripsi data lokasi yang ada pada *database server* MeetApps ke bentuk *ciphertext* sehingga tidak dapat diketahui. Proses modifikasi CBC (*Cipher Block Chaining*) dapat mengembalikan *ciphertext* ke plainteks yang memuat data lokasi.

6. Daftar Pustaka

[1]. Samkay H, 2013. Appointment Management Dengan Memanfaatkan Integrasi Media Sosial Facebook dan Global Positioning System (GPS) pada Android.

[2]. Munir, Rinaldi, 2006. Kriptografi, Bandung: Informatika

[3]. Dewi Romalia dan Aprian Riki, 2012. Implementasi Mode Operasi *Cipher*Block (CBC) pada Pengamanan Data

[4]. Daemon, Joan, 1965, The design of Rijndael: AES - The Advanced Encryption Standard/Joan Daemen, Vincent Rijmen. Berlin: Springer.

[5]. Liwandouw, Vania B & Wowor, Alz Danny, 2015. *Desain Algoritma Berbasis Kubus Rubik dalam Perancangan Kriptografi Simetris*. Bandung : Prosiding Setisi.

[6]. Stinson, D. R., 1995, *Cryptography: Theory and Practice*. CRC Press, Boca Raton, London, Tokyo.